STATE OF ALABAMA

Information Technology Guideline

Guideline 600-05G1: Configuration Management Process

1. INTRODUCTION:

From a security point of view, configuration management (CM) provides assurance that the system in operation is the correct version (configuration) of the system and that any changes to be made are reviewed for security implications. A CM process should be implemented to ensure that changes take place in an identifiable and controlled environment and that they do not unintentionally degrade any of the system's properties, including its security.

2. OBJECTIVE:

Provide guidelines for developing organization or system-specific CM procedures.

3. SCOPE:

These guidelines may be applied to all State of Alabama employees, contractors, vendors, or business partners with access to State information systems; to all computer and network systems owned by and/or administered by State agencies, and to all platforms (operating systems), all computer sizes (personal computers through mainframes), and all application systems (whether developed in-house or purchased from third parties).

4. GUIDELINES:

Based on the recommendations of the National Institute of Standards and Technology (NIST) in Special Publication 800-100: Information Security Handbook: A Guide for Managers, the following guidelines should be used to implement a CM process for State of Alabama information systems.

4.1 CONFIGURATION MANAGEMENT PROCESS

Managing the configuration of an information system and providing a process for continuous monitoring are two key information security practices of the operations and maintenance phase of the system lifecycle.

The high-level CM process, depicted in Figure 4-1, identifies the steps required to ensure that all system changes are properly identified, evaluated, authorized, and implemented.

Figure 4-1: CM Process

Step 1: Identify Change

The first step of the CM process begins with a person or process associated with the information system identifying a need for a change. A change may consist of implementing a new feature, upgrading a system component or operating system, or applying the latest security patches. The need for a change may be identified by audit findings or other reviews or by individuals such as users, maintainers, or the system owner. Once the need for a change has been identified, a change request should be submitted to the appropriate decision-making body.

Step 2: Evaluate Change Request

After initiating a change request, the effects the change may have on the system or other interrelated systems must be evaluated. Conduct an impact analysis of the change to answer the following questions:

- Is the change technically correct, necessary, and feasible within system constraints?
- How does the change affect the performance or the security of the system?
- Were associated costs for implementing the change considered?

Step 3: Implementation Decision

Once the change has been evaluated and tested, management should take one of the following actions:

- Approve. Implementation is authorized and may occur at any time after the appropriate authorization has been documented.
- Deny. Immediate denial of the request regardless of circumstances and information provided.
- Defer. Implementation decision is postponed until further notice. In this situation, additional testing or analysis may be needed before a final decision can be made.

Step 4: Implement Approved Change Request

After the change has been approved for implementation it may be moved from the test environment into production. To provide a greater assurance that unapproved changes do not get implemented into production, personnel updating the production environment should always be separate from those individuals that developed the change.

Step 5: Continuous Monitoring

Information systems are typically in a constant state of migration with upgrades to hardware, software, or firmware and possible modifications to the surrounding environment of the system. Because changes to an information system can have a significant impact on the security of the system, the CM process calls for continuous system monitoring to ensure the system is operating as intended and that implemented changes do not adversely impact either the performance or security posture of the system.

Monitoring and reporting requirements are defined in applicable State policies/standards.

4.2 CONFIGURATION MANAGEMENT PROCEDURES

Effective agency CM policy and associated procedures are essential to ensure adequate consideration of the potential security impacts due to specific changes to an information system or its surrounding environment. Organizations should develop and document CM procedures that provide step-by-step details for identifying, evaluating, approving, implementing, and documenting system changes.

Procedures must ensure that changes to a system, changes to any interconnected systems, or changes to the network are accomplished in an organized manner with traceability and accountability and without detrimentally impacting confidentiality, integrity, or availability.

Procedures should formalize and document the following CM concepts:

- Version control: ensures system components associate with the appropriate system version
- Procedures for system components to undergo thorough review and testing prior to being introduced into a production environment
- Impact analysis of proposed system changes to the security of the information system
- Change review and approval process
- Procedures to ensure all supporting information system documentation accounts for any configuration modifications
- Procedures for configuration changes to an information system in an emergency situation

CM procedures may be created for a specific system (or set of systems) or organization-wide. The scope of the CM procedures should include all the information technology architectural components (including hardware, operating system, software applications, and network technologies) of the system or of all systems under the direct operational control of the organization.

4.3 CONFIGURATION MANAGEMENT ROLES AND RESPONSIBILITIES

Required CM roles and responsibilities are defined in State IT Policy 600-05: Configuration Management. They include the System Owner, CM Manager, Information Security Officer (ISO), Configuration Control Board, System Users, Developers, Testers, and System Administrators.

4.3.1 Configuration Control Board (CCB)

The CCB is a decision-making body that must review configuration change requests before they can be implemented. The CCB acts on those changes that would cause material or substantive changes to the system, including design specifications, budget (including lifecycle cost projections), interface characteristics with other systems, functionality, and security.

Each agency should form a CCB that includes representation from senior management, system owner, security, and system support personnel.

CM procedures should describe the CCB, its roles, responsibilities, and membership. The interaction between the CCB, project management, and agency management should also be described.

4.3.2 Organizational CM Roles

Organizations may designate additional positions/personnel to comprise the local CM group. The size of the CM group is dependent on a variety of factors, such as number of systems, system size, and system complexity. To provide direction and oversight for the CM process, the following roles and responsibilities may be added.

Configuration Management Advisory Boards

CM advisory boards, comprised of technical representatives from each system technology discipline, may recommend approval or disapproval to the CCB on proposed configuration changes to the systems baseline.

Configuration Infrastructure Assurance Officer (CIAO)

The CIAO is responsible for keeping abreast of agency mission requirements and tasks that affect CM issues. The CIAO is responsible for initiating and conducting a semi-annual review of the CM process with all staff principles, team leads, and advisory board members. Process reviews and coordination meetings should be documented.

Configuration Support Council (CSC)

The CSC, comprised of representation from the agencies functional elements and technical staff, is chartered to establish and maintain control of CM issues in the disciplines of systems and security. The CSC should review any changes to the system and security baseline based on parameters set by the CSC.

4.4 CONFIGURATION CONTROL

Configuration control is the systematic evaluation, coordination, approval or disapproval, and implementation of all proposed changes in the configuration of a configuration item after formal establishment of its baseline. Establishing an initial baseline of hardware, software, and firmware components for the information system and subsequently controlling and maintaining an accurate inventory of any changes to the system is the objective of CM.

4.4.1 Configuration Items

Configuration items (CI) are the products that are to be placed under configuration control. These products may include the following items:

- Management documentation describing the processes used to develop (or manage the development of) the system, such as the Needs Statement and the Project Plan (developed according to agency standards and procedures)
- Technical documentation or baselines describing the system (e.g., Functional Requirements Document)

- Software components (computer programs, operating systems and support tools)
- Data and database components (files and records that exist apart from software which access the contents of a database)
- Network components (if applicable)
- Hardware components (computer workstations, peripherals, servers and routers if applicable)
- Other components that management may wish to include at its discretion

CM procedures should describe the types of CI that will be managed. Also describe the means by which the release of all system CIs will be managed to ensure proper version control.

4.4.2 Baseline Identification

A baseline describes the technical characteristics of each CI. Baselines serve as technical control points in the system lifecycle for the evaluation of proposed changes to these technical characteristics. There are several baseline types that are relevant to different phases in the system lifecycle. They include:

- Functional or Requirements Baseline
- Design Baseline
- Development Baseline
- Product Baseline

The product baseline represents the end-system product as built by the developers and includes the following:

- System hardware, software, and firmware
- Design and specification documentation
- Manuals (user, operations, maintenance, etc.)
- Installation and conversion procedures
- All changes needed to resolve problems detected during system acceptance and release testing and any discrepancies between the system, its requirements, and design documentation

Additionally, the product baseline must also account for the security configuration baseline requirements for the system that addresses the technical, operational, and management security controls for the system.

The product baseline and all the approved changes or modifications made to the system since acceptance provide a current description of the system. This baseline description

should be maintained throughout the operations and maintenance phase of the system lifecycle.

Ideally, the standard hardware and software baseline configuration for a system will be established at the time of procurement. However, for existing systems in which this did not occur, agencies should define and document the baseline configuration and put into force a configuration management methodology.

CM procedures should describe the process by which the product baseline will be managed.

4.4.3 Configuration Status Accounting

Configuration Status Accounting (CSA) is the process that provides managers with the information to determine whether changes are being implemented as directed. As approved changes are implemented, this accounting process will record and file information concerning the appropriately modified software, hardware, and/or documentation. The accounting process is responsible for identifying and issuing the most current approved versions of the CM-controlled items to project participants.

Outline the processes in CM procedures and describe how captured information will be used to accomplish functions such as assuring that the software/system satisfies functional requirements, that security requirements are satisfied, and that testing is performed in accordance with test plans. Identify the format and contents of the status summary reports that will be produced by this process.

4.5 CONFIGURATION AUDITS

Configuration audits validate compliance of development or operational requirements by comparing the functioning system to its technical documentation. Audits certify that the design, development, and integration meet the system's technical requirements, that the system is accurately documented, and that the system does not include unauthorized changes. With complex systems, informal audits should be performed to minimize the impact on development/operations and to identify deficiencies as soon as possible. Deficiencies noted during the informal audit, as well as recommendations for any corrective actions, should be made available for CCB or management review.

4.5.1 Functional Configuration Audit

A functional configuration audit is a formal examination of test records to verify that functional characteristics of the system comply with its requirements.

4.5.2 Physical Configuration Audit

A physical configuration audit is a formal examination of each coded version of a configuration. It assesses the system's technical documentation for completeness and accuracy in describing the tested system and compares the tested system configuration with the operational system delivered to ensure the appropriate components were tested and to verify that the system complies with all applicable standards.

CM procedures should describe the type and number of audits to be conducted, which will be determined by the size and complexity of the system, and describe the process by which

configuration audits will be performed. Describe how the audit trail will be kept that identifies all changes implemented on approved baseline deliverables.

4.6 TRAINING

Train personnel assigned responsibility for performing CM activities in the objectives, procedures, and methods for performing their CM-related duties. Examples of CM training include the following:

- CM roles, responsibilities, and authority
- CM standards, procedures, and methods
- CM tools and their capabilities
- Measurement, analysis, and reporting

CM procedures should provide information regarding the content and scheduling of CM training to be conducted.

5. DEFINITIONS:

SECURITY CONTROLS: The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. Security controls are defined in NIST Special Publication 800-53: Recommended Security Controls for Federal Information Systems.

6. ADDITIONAL INFORMATION:

6.1 POLICY

Information Technology Policy 600-05: Configuration Management

6.2 RELATED DOCUMENTS

Information Technology Standard 670-02S1: Monitoring and Reporting

Signed by Art Bess, Assistant Director

7. DOCUMENT HISTORY:

Version	Release Date	Comments
Original	3/21/2008	